Boolean function complexity

Lecturer: *Nitin Saurabh* Meeting: 10

Scribe: *Nitin Saurabh* 26.06.2019

In the last lecture we saw that when a t-DNF f is hit with a p-random restriction ρ then the depth of the *canonical decision tree* for $f|_\rho$ is larger than k with probability at most $(7pt)^k$.

We now state different versions of switching lemma with a better constant. They all follow from the above statement (modulo the improved constant).

Theorem 1 (Switching lemma version 1)**.** *Let f be t-DNF (or, t-CNF) and ρ be a p-random restriction where $p \in [0,1]$. Then, for all $k > 0$,*

$$\Pr_\rho[\mathsf{D}^{\mathsf{dt}}(f|_\rho) \geq k] \leq (5pt)^k.$$

Let us denote the $\mathsf{dnf\text{-}width}(f)$ (resp., $\mathsf{cnf\text{-}width}(f)$) to be the minimal width of a DNF (resp., CNF) representing f. Recall the width of DNF (or, CNF) is the maximal term (or, clause) size in it.

Theorem 2 (Switching lemma version 2)**.** *Let f be t-DNF and ρ be a p-random restriction where $p \in [0,1]$. Then, for all $k > 0$,*

$$\Pr_\rho[\mathsf{cnf\text{-}width}(f|_\rho) \geq k] \leq (5pt)^k.$$

Similarly one can have an analogous version where we hit a t-CNF with a random restriction and bound the $\mathsf{dnf\text{-}width}$ of the restriction. We note another version where the degree of the restricted function is bounded.

Theorem 3 (Switching lemma version 3)**.** *Let f be t-DNF (or, t-CNF) and ρ be a p-random restriction where $p \in [0,1]$. Then, for all $k > 0$,*

$$\Pr_\rho[\mathsf{deg}(f|_\rho) \geq k] \leq (5pt)^k.$$

We now use switching lemma to prove an optimal lower bound for Parity_n against constant depth circuits.

1 Lower bound for Parity

Recall in Lecture 8 we constructed a circuit of size $O(n2^{n^{1/(d-1)}})$ and depth d that computes Parity_n. We now prove a matching lower bound of $2^{\Omega(n^{1/(d-1)})}$.

Theorem 4. *If a circuit of size s and depth d computes* Parity_n*. Then,*

$$s \geq 2^{\Omega\left(n^{\frac{1}{d-1}}\right)}.$$

Proof. Let C be a circuit of size s and depth d computing parity. We assume, wlog, that the circuit is alternating. That is, each layer has the same type of gates (either OR or AND) and two consecutive layers have different types of gates. The overall idea is to use the switching lemma to perform depth-reduction on C while making sure that not many variables are set by the restriction. In the process the circuit is reduced to depth 2 and still computes Parity or $\neg\,\mathsf{Parity}$ on the remaining variables. We then obtain a lower bound on the initial size by comparing the bottom fan-in of the reduced depth-2 circuit and the number of remaining variables. We now formalize this idea.

Step 0: We do some preprocessing to be able to effectively apply the switching lemma. In particular, we reduce the bottom fan-in of C. That is, fan-in of the gates at layer 1. We want to make sure that the bottom fan-in of C is at most $4\log s$. To do so we hit C with p-random restriction where p is a constant. (Think of $p \leq 1/50$.) Thus, the probability that a gate of fan-in more than $4\log s$ is not set to a constant is at most

$$\left(\frac{1+p}{2}\right)^{4\log s} < \frac{1}{s^2}.$$

Therefore the probability that some gate of fan-in more than $4\log s$ survives is at most $1/s$ by the union bound.

Simultaneously the expected number of remaining variables is pn under the random restriction. Therefore, by Markov's inequality, with probability at least $1/2$, the number of remaining variables is at least $pn/2$.

Therefore, there exists a p-random restriction ρ such that the bottom fan-in of $C|_\rho$ is at most $4\log s$ and the number of unset variables is at least $pn/2$. Let us denote the restricted circuit $C|_\rho$ by C_0.

Step 1: We now hit C_0 with a p'-random restriction where $p' = p/\log s$ to reduce the depth by 1. Suppose, wlog, that layer 1 gates in C_0 are AND gates, so the layer 2 gates are OR gates and layer 3 gates are again AND gates. Now consider the gates at layer 2. Each gate is a DNF with width at most $4\log s$. Thus, when we hit this gate with p'-random restriction and use Theorem 2 with $t = k = 4\log s$, then we obtain a $(4\log s)$-CNF for the restricted function with probability at least $1 - (5p't)^k$. From the choice of p', t and k, we obtain

$$(5p't)^k \leq (20p)^k < 2^{-k} \leq \frac{1}{s^4}.$$

Thus the probability that some gate at layer 2 fails to switch to a CNF with small width is at most $1/s^3$. Also, again by Markov's inequality, with prob. at least $1/2$, the number of remaining variables is at least $(p' \cdot pn)/4 = (p^2 \cdot n)/(2^2 \cdot \log s)$.

Therefore, there exists a p'-random restriction ρ_1 such that it switches every gate at layer 2 by a CNF of width at most $4\log s$, thus reducing the depth by 1 (since layer 2 and 3

have same type of gates), and the number of unset variables is at least $\frac{p^2 \cdot n}{2^2 \cdot \log s}$. Let us denote the restricted circuit $C_0|_{\rho'}$ of depth $d-1$ by C_1.

We now recursively apply Step 1 to obtain a depth-2 circuit in $d-2$ steps as follows.

restriction	circuit	bottom fan-in	depth	# remaining variables
	C	n	d	n
p-restriction	C_0	$4 \log s$	d	$\frac{pn}{2}$
p'-restriction	C_1	$4 \log s$	$d-1$	$\frac{p^2 \cdot n}{2^2 \cdot \log s}$
p'-restriction	C_2	$4 \log s$	$d-2$	$\frac{p^3 \cdot n}{2^3 \cdot (\log s)^2}$
$\vdots$ $\vdots$	$\vdots$ $\vdots$	$\vdots$ $\vdots$	$\vdots$ $\vdots$	$\vdots$ $\vdots$
p'-restriction	C_{d-2}	$4 \log s$	2	$\frac{p^{d-1} \cdot n}{2^{d-1} \cdot (\log s)^{d-2}}$

Thus, in the process we have obtained a depth-2 circuit with width at most $4 \log s$ computing Parity or $\neg \mathsf{Parity}$ on at least $\frac{p^{d-1} \cdot n}{2^{d-1} \cdot (\log s)^{d-2}}$ variables. Hence, we must have

$$4 \log s \geq \frac{p^{d-1} \cdot n}{2^{d-1} \cdot (\log s)^{d-2}},$$

and thereby,

$$(\log s)^{d-1} \geq \frac{p^{d-1}}{2^{d-1} \cdot 4} \cdot n.$$

This implies the required lower bound on s. □

2 Upper bound on a minimal certificate size

Recall the certificate complexity $\mathsf{Cert}(f)$ of a function f is $\max_x \mathsf{Cert}(f, x)$. We now define a new measure called the *minimal certificate* complexity $\mathsf{Cert}_{\min}(f)$ of f as follows, $\mathsf{Cert}_{\min}(f) := \min_x \mathsf{Cert}(f, x)$. By definition $\mathsf{Cert}_{\min}(f)$ is the minimum number of bits that must be set to make f a constant. We now show that constant depth circuits have low minimal certificate.

Theorem 5. *Let f be computable by a circuit of size s and depth d. Then,*

$$\mathsf{Cert}_{\min}(f) \leq n - \frac{n}{c_d \cdot (\log s)^{d-2}} + 4 \log s,$$

where c_d is a constant that depends on the depth d.

Proof. Consider the depth reduction process in the proof of Theorem 4. At the end, we obtained a circuit C_{d-2} of depth-2 with bottom fan-in $4 \log s$. To obtain this circuit we set at most $n - \frac{n}{c_d \cdot (\log s)^{d-2}}$ variables. Now observe that any depth-2 circuit can be made constant by setting all the variables in any one term (or, clause). Therefore, we need to set at most $4 \log s$ more variables to make C_{d-2} a constant, and thereby obtaining the theorem. □

Note we could also obtain the lower bound for parity from the above theorem since $\mathsf{Cert}_{\min}(\mathsf{Parity}_n) = n$.

3 Fourier transform of constant depth circuits

In the next lecture we will prove the following structure theorem on the Fourier spectrum of a function computed by constant depth circuits.

Theorem 6. *let f be function computed by a circuit of size s and depth d. Further let $k > 0$. Then,*

$$\sum_{S \subseteq [n] \colon |S| > k} \widehat{f}(S)^2 \leq 2 \cdot s \cdot 2^{-k^{1/d}/20}.$$